THE CHALLENGE

How will you defend your organization...and yourself?

CORE Corporation
Founder and CEO

WAYNE SHAW

YOU ARE ON THE HOT SEAT

Murphy's Law—"Anything that can go wrong will go wrong"—may *sound* right.

And it *feels* safer to delegate cybersecurity decisions to techies.

But the fact is that far more incidents *can* happen than *will* happen.

So, you might overspend to defend against incidents that only "can" happen while leaving yourself wide open to incidents that "will" happen. And because techies are not fiduciaries, you are left liable for their decisions.

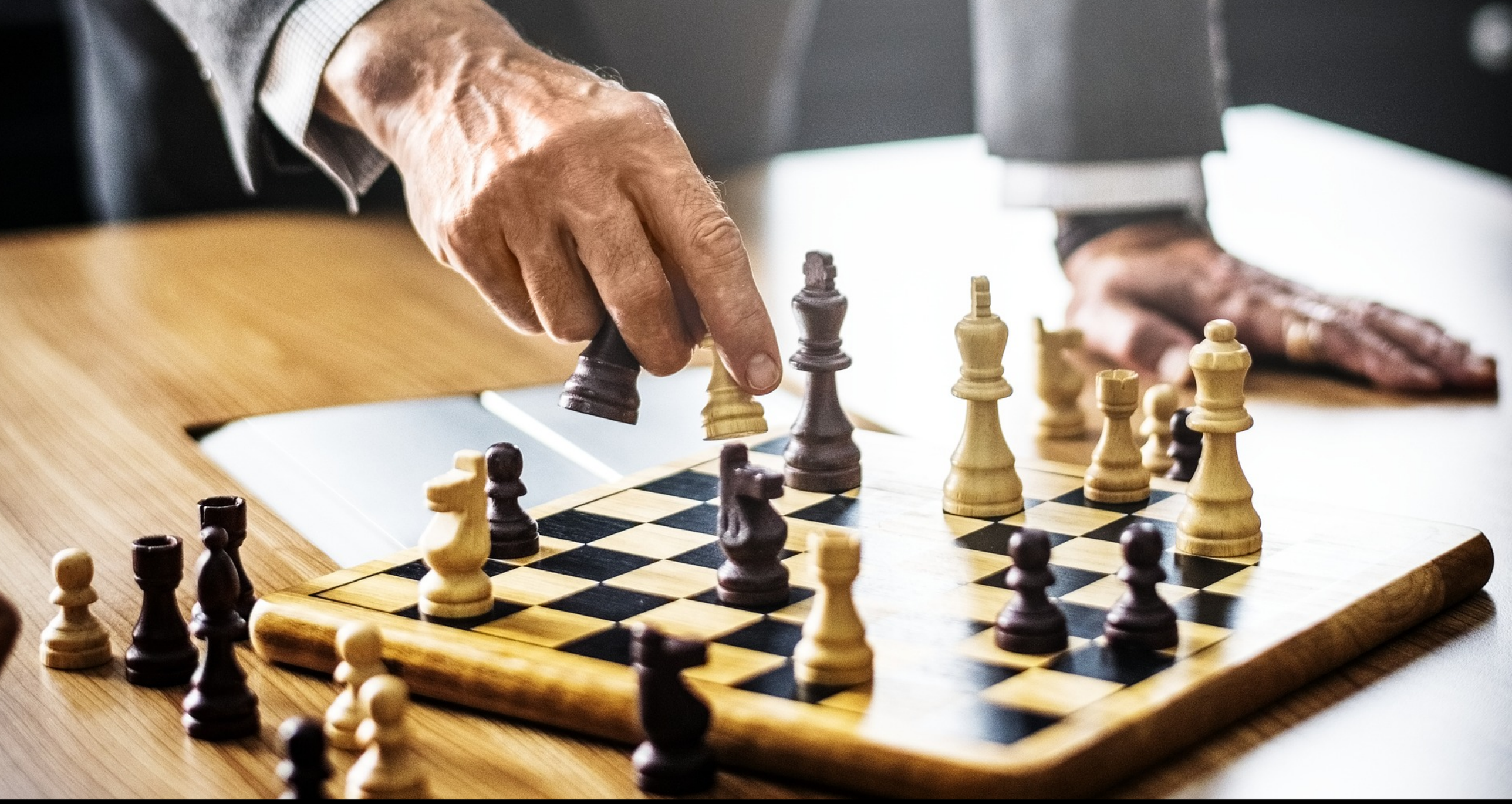
CORE offers you a solution to your problem.

Wayne Ignatius Shaw
CEO

Wayne Shaw, Founder &
CEO CORE Corporation

CORE

Helping you to make the best leadership decisions about your cyber defenses



CORE CYBER COMMAND®

For top management and their organizations

CORE EMPOWERS YOU

No matter how much you spend on cybersecurity or how brilliant your people are, you ***will*** be hacked.

The secret to taking command of this situation is by understanding how to tolerate a certain number and kind of incidents, while blocking everything else. Core empowers you —the top management of organizations—to manage cyber risk and protection correctly.

CORE helps you to understand your unique vulnerabilities so you can invest where it counts and not overspend where it doesn't.

"HOW MUCH SHOULD I SPEND ON CYBER DEFENSES?"

How much you spend on cyber defense measures is a strategic business decision of the top management of an organization.

We use the "CORE Method" to help you to frame the problem correctly and helps you to answer this central strategic question. And this must be done before you spend a penny on any cybersecurity measures.

THE CORE METHOD

"Strategy comes before tech decisions!"

Step 1: What regulations apply to you?

CORE starts by analyzing the cyber laws and regulations to determine which ones apply to you. CORE's analysis is specific to your organization's activities and industry, which reduces the risk of you trying to comply with regulations that do not apply to you while missing the ones that do.

CORE combines legal and compliance expertise with practical process knowledge, technical expertise, and industry-specific expertise to filter the regulations for you real-world situation.

Our expertise covers different regulatory jurisdictions, such as the US, Japan, Hong Kong, and elsewhere:

- Japan: "APPI", "PIPL" "TBA," "UCAL," Unfair Competition Protection Act, Basic Act on Cybersecurity
- Hong Kong: "Cap" 200, 106
- USA: "CFAA," "ECPA"
- Singapore: "CMA"
- And many others

Step 2: How much can you tolerate?

How many incidents are you willing to tolerate? Of what type? And of what cost?

It is a strategic tradeoff that only the top management can make because they bear liability for the result. And because penetrating is certain, the tradeoff always exists, whether or not people accept its existence.

CORE helps you to find an answer to the tradeoff that is practical for your case.

We help you to create an accurate business case: a custom "Cyber Defense Investment Plan" that is unique to you. It is your playbook for integrating cyber defense measures into your organization—management, governance, people, processes, and technology—along with the costs and benefits for each one.

CORE creates scenarios about the estimated costs from litigation, regulatory penalties, and/or court settlements for certain incidents. We consider your budget, the technical ability of your organization, and the spectrum of threats from outside your organization...and from within. Then we map it to the cyber defense investments in people, processes, systems that you need to make to get the best value.

Step 3: How will you lead?

Overseeing the implementation of your cyber defenses need not be complicated. CORE recommends guidelines for top management and fiduciaries and coaches them so they can properly perform their own duties regarding mitigation, management, and response to incidents.

Now, you are ready for the technology part!

At this point, you are well-positioned to allow your technical personnel to undertake the design and implementation of your cyber defense measures.

This is where "CORE Execution Services" comes in: helping your technical and operational people execute your Cyber Defense Investment Plan. Learn more about "CORE Execution Services" in the next section.

* * *

CORE DEFENSE SERVICES®

For the CIO, CTO, and CISO

CORE HELPS THE CIO, CTO, & CISO TO EXECUTE

CORE helps the CIO and CISO to zero-in on practical, relevant solutions for integrating the appropriate cyber resilience into the company's management, governance, and technology within the budget and the time-frame that have been specified by the top management in their Cyber Defense Investment Plan.

Activities include, for example, the design, construction, staffing, and initial operations of a new Security Operations Center (SOC), or renovation of an existing one. It also covers the creation of procedures, responses, and remediations—in other words, resilience—*after* an incident occurs to ensure business continuity.

Training is a pillar of excellent implementation. CORE trains employees and vendors in the client's company. Training might be a skills brush-up for the CISO, hardcore in-service training for an engineer, or general awareness training for regular non-technical employees.

CORE brings together decades of industry experience in cybersecurity from multinational corporations, government and military, and the auditing community. We are experts at protecting critical systems, data and networks worldwide.

MENU OF CORE DEFENSE SERVICES®

1. CyberStorm® - cybersecurity forensics & assessments
2. CyberShield® - staff training
3. CyberDrill® - simulated attack
4. Penetration/Intrusion Testing
5. Digital Forensics and Incident Response (DFIR)
6. CORESOC® - security operations center
7. "No Phish!"® by Core - managed phishing service
8. CORE Cyber Expert Resources
9. CORE MSSP - managed security service

DESCRIPTIONS OF CORE DEFENSE SERVICES®

1. CyberStorm®

Whether you suspect you have been hacked or are wondering about your preparedness for a hack, start protecting your business with the most advanced cybersecurity forensics and assessments of their kind.

Whether for internal use only or for use in court, CyberStorm® by CORE aids clients to visualize and understand their current level of noncompliance, gaps, and risks, and to develop mitigating measures and controls to address and monitor them.

CyberStorm® by CORE provides you insight into unseen cyber-dangers lurking within your business. By uncovering and resolving the vulnerabilities that demand immediate action,

you'll be able to confidently continue with business operations without fear of attacks from cyber-space.

CyberStorm® by CORE digs deep into your infrastructure and technology spectrum, enabling you to discover issues before they become a problem, and helps you to track down evidence when a problem has occurred.

2. CyberShield®

Go beyond cybersecurity and build a culture of awareness and cyber resilience throughout your organization for the long-term. CyberShield® by CORE helps your employees and vendors to take a strong step forward to acquiring a responsible security-mindset by means of threat awareness training. It also demonstrates to regulators that you are taking sincere and reasonable measures in this regard.

CyberShield® by CORE delivers tangible results quickly and cost-effectively.

Many companies are lacking in this basic and fundamental responsibility, either due to lack of resources, skill-set, or both. For an organization to effectively implement cybersecurity company-wide, the first line of defense is to ensure each and every employee is made aware of the company's internal security standards and policies and their role for cybersecurity within the organization. Regulators and auditors are not sympathetic to organizations that do not meet this basic requirement. Too often such a gap is a costly one.

Organizations should ensure that their employees understand the company's security standards. This, in turn, aids in protecting the company if and when a situation occurs involving incidents such as unauthorized access or breaches.

Our cybersecurity gap analysis digs deep into your infrastructure and technology spectrum, enabling you to discover issues before they become a problem.

3. CyberDrill®

What would you do if your company website was attacked today? How would you and your team react?

A large percentage of companies that have been attacked have divulged that they had never conducted a "Cybersecurity" drill. Many of these companies had to close as a result of, in part, their unpreparedness to recover from a cyber-attack.

CyberDrill® by CORE will boost your readiness. You will be able to answer important those important questions and have a clear path forward and useful data for undertaking practical actions to address any gaps.

Enterprises have deployed multiple technologies and processes for detecting and responding to threats. When it comes to responding to real security incidents, however, many organizations fail.

Conducting CyberDrill® by CORE periodically is an essential component of cybersecurity preparedness and cyber resilience. It tests all elements and components for effective incident detection and response strategy.

CORE aids customers to draft real-life scenarios to suit their business strategies, needs, and capabilities. With CyberDrill®

by CORE, you can test your controls before Hackers test them for you.

4. Penetration/Intrusion Testing

Internet-borne attacks have become increasingly more sophisticated. Weaponized malware and viruses have become the norm. Businesses can be robbed of confidential or proprietary information. Internet-facing systems need to be strengthened in order to protect business and customer information.

Conducting an Intrusion test of your company's infrastructure, critical systems and applications is an effective approach to ensuring your network and critical systems are not infiltrated or vulnerable to malware and hackers.

Intrusion Testing enables companies to detect, identify, assess and mitigate vulnerabilities that would otherwise expose the enterprise to risks, internally and externally.

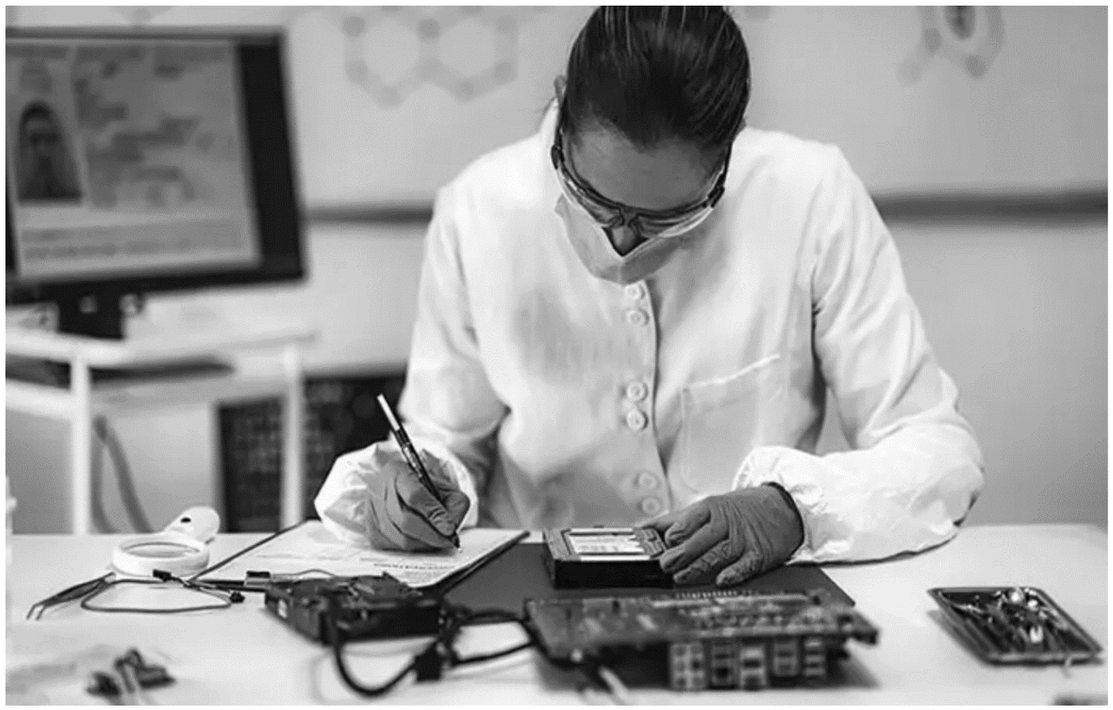
environment with our Enterprise Digital Rights Management solution, which is compliant to requirements such as GDPR, NIST, and FSA.

5. Digital Forensics Investigation and Incident Response (DFIR)

Our Digital Forensics Investigation service aid clients to unravel the digital truth behind how, who and why an attack happened.

This is a complex, time consuming, and time critical process that requires know-how and in-dept knowledge of cybercriminals. CORE's Digital Forensics Investigators with extensive expierence in the digital forensic field, provide the expertise that enables our client to uncover how their business was targeted.

We work covertly to protect our clients identity,businesses and to uncover the digital details behind the attack to include who is responsible and exactly what was taken.



6. Security Operations Center (SOC): CORESOC®

The Security Operations Centers (SOC) is an integral part of an effective business strategy. Developing the right plan, and the team to implement it is crucial. CORE team of SOC specialists can develop and implement the right strategy for your business. With CORSOC®, you will have a SOC that meets or exceeds what is required in the business case and world-class excellence of cyber monitoring and defense.

7. Managed Phishing Service: “No Phish!”® by CORE

CORE provides a Managed Phishing Service (PhaaS). Called “No Phish! by CORE, our team of experts will go to work creating and executing phishing simulation tests, along with awareness training. When time is of the essence, we can get your company up and rolling in matter of days.

8. CORE Cyber Expert Resources

For companies that do not have enough internal cybersecurity resources to support their organizations, they rely on employees to do double duty: their normal job plus cybersecurity activities. This puts the organization in a very risky situation.

Enjoy the expertise and efficiency of CORE security resources on a consignment basis. Our cybersecurity resources can help you to fulfill your security obligations.

9. Managed Security Service Provider: CORE MSSP

CORE provides its services that are relevant to your needs in the form of a bundled packaged, known as CORE MSSP. On a retenion basis, CORE provides comprehensive cyber security services to aid clients in the protection of their business. Your package is customized made and covers at a basic level the areas that are most popular with our clients: Security resources, Vulnerability Assessments, Awareness Training, Security Audit, Penetration Testing, Managing Security Projects and more.

* * *

Our Company

CORE

- The most reliable cyber defense for top management and their organizations
- Provides integrated expertise in law, strategy and governance, technology, processes, and industry
- CORE's professionals have a minimum of 20 years experience each.
- Multidisciplinary, multilingual, and multicultural
- Advanced Penetration Testing certified, Web Application certified, CCNA certified, CompTIA Network+, CISSP, ISC2 Cloud Security certified, Cryptography certified, Python Security professionals certified, CompTIA Security+ certified and Certified Ethical Hacking (CEH) certified

BOARD OF DIRECTORS

Mr. Wayne Shaw, Mr. Babak Esmaeili, Ms. Mio Kazuko, Mr. Terrie Lloyd

REPRESENTATIVE DIRECTOR

Mr. Wayne Shaw, Founder and CEO

NATURE OF BUSINESS

Private stock company
Bank of Record: Mizuho Bank, Tokyo
Paid-in-Capital: JPY10,000,000

Activities
Information and Cyber Security
Technology and Services

CONTACT

CORE, K.K.
Yebisu Garden Place Tower 18F, Ebisu 4-20-3, Shibuya-ku Tokyo 150-6018
Email: info [at] coresecurity [dot] co [dot] jp